AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

INFORMATION IN THREE SERVERS DESCRIBED IN ATTACHMENT A, STORED AT PREMISES CONTROLLED BY NEWFOLD DIGITAL, INC.

Case No. 3:23-sw- 75

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:
See Attachment A.

located in the Middle District of Florida, there is now concealed *(identify the person or describe the property to be seized)*:
See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 1343	Wire Fraud
18 U.S.C. § 1956	Laundering of monetary instruments

The application is based on these facts:
See Attached Affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Steele D. Holland
Applicant's signature

Steele Holland, Task Force Officer, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: May 18, 2023

/s/ MRC
Mark R. Colombell
United States Magistrate Judge
Judge's signature

City and state: Richmond, Virginia

Honorable Mark R. Colombell, Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

IN THE MATTER OF THE SEARCH OF INFORMATION IN THREE SERVERS DESCRIBED IN ATTACHMENT A, STORED AT PREMISES CONTROLLED BY NEWFOLD DIGITAL, INC.

Case No. 3:23-sw-75

Filed Under Seal

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Steele Holland, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises controlled by Newfold Digital, Inc. f/k/a The Endurance International Group, Inc. (hereafter "Newfold Digital"), an email provider headquartered at 5335 Gate Parkway, 2nd Floor, Jacksonville, Florida 32256. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Newfold Digital to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Task Force Officer of the Federal Bureau of Investigation (FBI) assigned to the Richmond Division and detailed from the Virginia Department of State Police. I became a Task Force Officer with the FBI in March 2015. I am currently assigned to the Cyber Squad

within the Richmond Division where I am primarily responsible for the investigation of cyber matters, which include computer-enabled criminal violations relating to computer enabled fraud designed to induce victims to wire money to criminally controlled bank accounts. Before becoming a Task Force Officer, I was assigned as a Special Agent with the Virginia Department of State Police starting in January 2014. In that role, I received and distributed intelligence material to appropriate parties and provided field support by way of actionable intelligence. Prior to my role as a Special Agent, I was a uniformed state trooper with the Virginia Department of State Police, beginning in January 2003. Throughout my employment as a police officer, I conducted criminal investigations and I have received many classes in basic and advanced criminal investigation techniques. As a Task Force Officer with the FBI, I have received training in the investigation of cases involving computer crimes and the use of computers to advance criminal schemes.

3. As a Task Force Officer of the FBI, I am authorized to conduct investigations, carry firearms, execute warrants, make arrests for offenses against the United States and perform other such duties as are authorized by the FBI. Through the course of these investigations, I have conducted interviews and secured other relevant information using a variety of investigative techniques.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of federal criminal law, specifically wire fraud (18

U.S.C. § 1343) and money laundering (18 U.S.C. § 1956) are associated with servers identified by the following IP addresses:

- 162.144.78.100 (TARGET ADDRESS 1)
- 162.144.78.186 (TARGET ADDRESS 2)
- 192.163.212.109 (TARGET ADDRESS 3)
- 142.4.2.128 (TARGET ADDRESS 4)
- 192.163.212.110 (TARGET ADDRESS 5)
- 142.4.0.84 (TARGET ADDRESS 6)
- 142.4.0.45 (TARGET ADDRESS 7)
- 142.4.11.163 (TARGET ADDRESS 8)

There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. *See* 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

RELEVANT STATUTORY PROVISIONS

6. Title 18, United States Code, Section 1343 (wire fraud) provides:

> Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined under this title or imprisoned not more than 20

years, or both.

7. Money laundering as set forth in 18 U.S.C. § 1956 is described in pertinent part as follows:

> (a)(1) Whoever, knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, conducts or attempts to conduct such a financial transaction which in fact involves the proceeds of specified unlawful activity—
>
> (A)(i) with the intent to promote the carrying on of specified unlawful activity; *or*
>
> * * *
>
> (b) knowing that the transaction is designed in whole or in part—
>
> (i) to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity;
>
> * * *
>
> shall be sentenced to a fine of not more than $500,000 or twice the value of the property involved in the transaction, whichever is greater, or imprisonment for not more than twenty years, or both.

PROBABLE CAUSE

8. The United States is investigating the unauthorized access of Amazon seller accounts and subsequent changing of the associated banking information, resulting in Amazon disbursements to those sellers being redirected to foreign bank accounts. This fraud happened in two stages. In the first stage of this fraud, subjects conducted a phishing campaign, where they used Gmail accounts to spoof Amazon emails. These phishing emails were designed to compromise the login credentials of Amazon sellers. In the second stage, the subjects used Amazon Web Services ("AWS") accounts to log into the seller accounts and to change the seller's disbursement bank account to a foreign bank account controlled by the subjects. Several of the AWS accounts established and used by the subjects had Gmail addresses associated with them.

Amazon Background

9. Amazon is an online retailer headquartered in Seattle, Washington. Among other

businesses, Amazon runs widely known e-commerce websites. Amazon calls these websites "stores." Amazon offers products for sale in its stores that are sold by Amazon itself, and products that are sold by third-party sellers.

10. Each third-party seller must create a unique account with Amazon. To create a third-party seller account, users must provide Amazon with a variety of information and documentation, including a government-issued ID, tax information, and a phone number. Sellers must also provide a financial account so that Amazon may disburse funds owed to the seller through sales made on Amazon's stores. A seller may update this financial account at any time. Sellers are able to use virtual bank accounts through companies like Hyperwallet, which, among other things, facilitate currency transfers not otherwise supported by Amazon. Approximately every 14 days, Amazon disburses funds from the third-party seller's Amazon account to the seller's account on file.

11. Amazon also operates the subsidiary Amazon Web Services, Inc., which provides cloud computing services, including Amazon Elastic Compute Cloud ("EC2"), a scalable service that allows users to rent virtual computers on which to run computer applications. Each AWS customer must create a unique account with Amazon by providing Amazon with information, including an email address, phone number, and payment method.

Initial Complaint

12. On November 24, 2020, a company official of West End Toys, LLC, an online toy seller based in Richmond, determined that the company's Amazon account was compromised and that a bi-weekly payment was redirected to an unknown bank account ending in 629. However, Amazon was later able to stop the disbursement and return the funds to West End Toys, LLC. The attempted losses due to the fraud were $176,469.62.

13. The company official advised that a week prior, West End Toys had received a phishing message and that one of his employees had responded and provided the company's telephone number associated with its Amazon account. Additionally, this employee received a second message and clicked on a hypertext "button" contained in it. Analysis by investigators of the email header revealed this message was sent from IP address 74.208.4.194.

14. On November 24, 2020, Amazon provided the FBI with the following information regarding the bank account to which the subjects attempted to redirect the funds:

- Routing number: 073972181
- Account number: 4452757076629

15. In examining the West End Toys account's sign-in history, Amazon determined that West End Toys' account was accessed on November 17, 2020. After this access, the email address on the account was changed to lwestendtoys@gmail.com, which added an "l" to the beginning of the legitimate seller email address already on the account. The bank account was also updated to the account ending in 629, which was the destination for the fraudulent disbursement cancelled on November 24, 2020.

How the West End Toys Account was Compromised

16. West End Toys received two emails on November 17, 2020, sent to their westendtoys@gmail.com address. In the first message, allegedly sent by Seller Notification, seller-notification@www-amazon.com, they were informed that Amazon was unable to verify some of the information in their seller account. These emails instructed West End Toys to log into their Amazon Seller Central account, locate the emergency notification section, and to enter a valid phone number. Once this was completed, they were to reply within 24 hours with a confirmation email and they would be sent a verification email to confirm the update as the

principal account owner. A review of the message header revealed that the "Reply-To" address was seller-performance@8cnzvfen-amazon.com.

17. A few minutes later, West End Toys received a message that appeared to be from seller-performance@amazon.com, which was actually a masked email address that hid the actual address of seller-performance@8cnzvfen-amazon.com. A Whois query for the domain[1] "8cnzvfen-amazon.com" revealed that the mail exchange (MX) records resolved to New Fold Digital.com (in other words, an email account associated with New Fold Digital). This message thanked West End Toys for their confirmation email and instructed them to click on a "Complete Review" button in the email to confirm the update of their phone number as principal account owner. This button contained a hyperlink that connected to https://www.New Fold Digital.com/url?q=https://sellercentral.amazn.com-594040.eu/ap/en/view?c3e72d83-9e52-442d-8c73-376ad760aff9&sa=D&sntz=1&usg=AFQjCNGgeM1cmh22ib3LZaXlsjhYnCU5fQ. Investigators determined that these messages were received and the "Complete Review" button was clicked on by one of West End Toy's employees.

18. On November 26, 2020, November 30, 2020, and December 1, 2020, West End Toys received three additional emails. Each of these was sent as a reply to the confirmation email Jones had sent to the original phishing message confirming their phone number. These messages appeared to be from either Seller Notification or seller-performance@amazon.com, but each

[1] A domain name locates an organization or other entity on the Internet. For example, the domain name "www.example.com" locates an Internet address for "example.com" at a specific Internet point (Internet Protocol ("IP") address) and a particular host server named "www." The "com" part of the domain name reflects the purpose of the organization or entity and is referred to as the "top-level domain name." The "example" part of the domain name defines the organization or entity and together with the top-level is referred to as the "second-level domain name."

actually came from seller-performance@8cnzvfen-amazon.com. Additionally, the content of these emails was similar, with each claiming an issue had been found with West End Toys' seller account that needed to be addressed immediately and including a "Fix Issue" button. The hyperlink for each of these buttons was directed to https://www.New Fold Digital.com/url?q=https://sellercentral.amazn.com-492950.eu/ap/en/view?df0de9d4-0954-4962-b1af-66358eb64805&sa=D&sntz=1&usg=AFQjCNHL3-HT8ubN-Oc-cdal6EM2pC-P1w.

19. On December 2, 2020, FBI agents examined the laptop computer that the West End Toys employee had used to click the link in the second email and conducted a memory capture. A review of this memory capture did not identify any indicators for the presence of malware. On December 15, 2020, the FBI Richmond Division's computer scientist opened the second email received by West End Toys and clicked on the "Complete Review" button and was redirected to https://sellercentral.amazon.com-f3xy8od3.eu. This website had the appearance of Amazon Seller Central and included a login prompt. When false login information was entered, a confirmation prompt was displayed asking that the login information be reentered, with an additional CAPTCHA.

How the Optique Elegance Optique, LLC Account was Compromised

20. On April 8, 2021, an individual identified herein as "A.E." filed a fraud complaint on behalf of Optique Elegance Optique, LLC (Optique), which is an Amazon seller, with the Internet Crime Complaint Center (IC3) through its website, www.ic3.gov. According to the ic3.gov complaint, on February 25, 2021, Optique received a phishing message that appeared to be from Amazon. This email requested that Optique verify the last four digits of their primary phone number. An Optique employee responded to the email and provided the last four digits of its primary phone number as requested.

21. Optique then received a subsequent phishing email that requested that they login to their Amazon seller account and verify their security settings. The phishing email provided URL https://sellercentral.amazon.com.735783.info/1c3db464/6934-4a78-8470-128f90dffca4 to complete its requested task.

22. On March 23, 2023, Optique expected to receive an Amazon disbursement in the amount of $199,770.19. Minutes before the deposit was initiated, Optique received an email in Korean that stated that the bank account on file had been changed. Optique routinely received all of its emails from Amazon in English. Three days later, on March 26, 2023, Optique realized that the language change in emails from Amazon was part of a scam that resulted in its $199,770.19 disbursement being redirected to an unknown bank account ending in "671" and having a transfer ID of 091000013830324.

How the Wonita International, Inc. Account was Compromised

23. On December 6, 2022, an individual identified herein as "H.Z." filed a fraud complaint on behalf of Wonita International, DBA Danzia (Danzia), an Amazon seller, with the Internet Crime Complaint Center (IC3) through its website, www.ic3.gov. On November 15, 2022, Danzia received a phishing email that appeared to be from Amazon. This email requested that Danzia verify its mobile phone number on its Amazon Seller Central account, and provided a "Verify Now" button that linked to a webpage that looked identical to Amazon's actual Seller Central page.

24. The phishing message stated, "Hello from Amazon, [y]ou are receiving this message because you need to verify the primary mobile phone number associated with your Amazon account. Within 24 hours of this email, please complete this verification step to avoid unnecessary disruption to your selling account."

25. The "Verify Now" button included in the email linked to: https://www.New Fold Digital.com/url?q=https%3A%2F%2Fsellercentral.amazon.com-f5b4en.me%2Fap%2Fcvf%2Frequest%2Farb%3Ddeb0c8a9-c3c9-4c0f-be70-50ca4a8e077f&sa=D&sntz=1&usg=AOvVaw01CBftTZCtPICWthmDMEHf.

26. Danzia reported that at the time they received the message, this button redirected them to "sellercentral.amazon.com-ws.me."

27. Danzia provided its username and password to login, not realizing it was a fake webpage. After unwittingly providing their username and password, Danzia's $82,051.91 Amazon disbursement scheduled for November 28, 2022, was redirected to an unknown bank account ending in "210" in Spain.

28. A Whois query on domaintools.com of the domains used to carry out each of the compromises described in paragraphs 14-29 revealed that the domains resolved to servers[2] managed by Newfold Digital, Inc. The servers were associated with IP addresses 162.144.78.100 (TARGET ADDRESS 1), 162.144.78.186 (TARGET ADDRESS 2), and 192.163.212.109 (TARGET ADDRESS 3).

29. On April 10, 2023, domaintools.com queries for historical Domain Name System (DNS) data were conducted on the TARGET ADDRESSES. These queries revealed that multiple

[2] A server is a computer or program dedicated to providing services to other computers or programs, referred to as 'clients'. DNS clients, which are built into most modern desktop and mobile operating systems, enable web browsers to interact with DNS servers. Servers are assigned specific IP addresses when they are connected to the internet. A domain registrar maps those IP addresses to domains created and registered on the registrar's infrastructure.

domains resolved to the same IP addresses from 2020 through the present. These domains included the following:

a. sellercentral.amazn.com-594040.eu (resolved to TARGET ADDRESS 1 and TARGET ADDRESS 2), which was the domain associated with the "Complete Review" button used in the phishing email targeting West End Toys discussed in paragraph 19 above;

b. sellercentral.amazon.com.735783.info (resolved to TARGET ADDRESS 1 and TARGET ADDRESS 2), which was the domain used in the phishing email targeting Optique discussed in paragraph 23 above;

c. sellercentral.amazon.com-f5b4en.me (resolved to TARGET ADDRESS 1 and TARGET ADDRESS 2), which was the domain used in the phishing email targeting Danzia discussed in paragraph 27 above; and

d. sellercentral.amazon.com-ws.me (resolved to TARGET ADDRESS 3), which was the domain associated with the "Verify Now" button used in the phishing attempt targeting Danzia discussed in paragraph 28 above.

30. Based on the similar naming convention, it is highly likely that the domains were used in other phishing schemes that redirected other victims to the credential harvesting services hosted at the TARGET ADDRESSES. Each domain resolved, at different times, to both TARGET ADDRESS 1 and TARGET ADDRESS 2, or to TARGET ADDRESS 3.

31. The naming convention used in the majority of the domains that pointed to TARGET ADDRESS 1 began with "sellercentral-amazon.com-[six alph-numeric characters]" or "go.amazonsellerservice.com-[six alph-numeric characters]." The naming convention used by domains that pointed to TARGET ADDRESS 2 included "com-[six numbers]," "sellercentral-

europe.amazon.[six numbers]," "sellercentral.amazon.com-[six numbers]," "[six number].com-[six numbers]," or "[six number].info." A large number of other domains using these naming conventions also resolved to the TARGET ADDRESSES between September 2020 and the present.

32. Records from Newfold Digital indicated that the subscriber for TARGET ADDRESS 1 and TARGET ADDRESS 2 was also the subscriber listed for a server identified by IP address 142.4.2.128 (TARGET ADDRESS 4).

33. Newfold Digital records also indicated that the subscriber for TARGET ADDRESS 3 was the subscriber listed for servers identified by IP addresses 192.163.212.110 (TARGET ADDRESS 5), 142.4.0.84 (TARGET ADDRESS 6), 142.4.0.45 (TARGET ADDRESS 7), and 142.4.11.163 (TARGET ADDRESS 8).

34. A shodan.io query[3] for TARGET ADDRESS 1 and TARGET ADDRESS 3 identified the last recorded Secure Shell Protocol (SSH)[4] key fingerprint for TARGET ADDRESS 1 was 36:cc:68:e4:cb:81:12:c5:96:a4:f7:7f:3d:b6:e5:12 (SSH Key Fingerprint 1), and the latest recorded SSH key fingerprint for TARGET ADDRESS 3 was 89:b4:68:71:1f:ce:2a:85:fe:61:0e:d8:22:71:d8:59 (SSH Key Fingerprint 2).

---

[3] Shodan is a search engine for finding specific devices, and device types, that are connected to the Internet. Examples of the types of devices revealed in a Shodan search include servers, routers, and the large collection of devices like webcams, smart TVs, fitness trackers and other gadgets that are commonly referred to as "the Internet of Things (IoT)." A variety of data types, e.g., IP addresses, SSH public key fingerprints, etc., can be used to conduct Shodan queries.

[4] The Secure Shell Protocol (SSH) is a cryptographic network protocol for operating network services securely over an unsecured network. Its most notable applications are remote login and command-line execution. In very general lay terms, an SSH session creates an encrypted connection over the Internet between a remote user and a server. The encrypted connection prevents an unauthorized person from intercepting or eavesdropping on the contents of the data transmitted during this secure connection.

35. As detailed below, the shared SSH key fingerprints between TARGET ADDRESSES 1, 2, and 4 indicates that the same computers or individuals are behind the encrypted communications with the servers.

36. As detailed below, the shared SSH key fingerprints between TARGET ADDRESSES 3, 5, 6, 7, and 8 indicates that the same computers or individuals are behind the encrypted communications with them.

37. An additional shodan.io query for SSH Key Fingerprint 1 and SSH Key Fingerprint 2 revealed that both SSH key fingerprints were shared with the other target accounts as follows:

- 162.144.78.100 (TARGET ADDRESS 1) (36:cc:68:e4:cb:81:12:c5:96:a4:f7:7f:3d:b6:e5:12) (SSH Key Fingerprint 1)
- 162.144.78.186 (TARGET ADDRESS 2) (36:cc:68:e4:cb:81:12:c5:96:a4:f7:7f:3d:b6:e5:12) (SSH Key Fingerprint 1)
- 192.163.212.109 (TARGET ADDRESS 3) (89:b4:68:71:1f:ce:2a:85:fe:61:0e:d8:22:71:d8:59) (SSH Key Fingerprint 2)
- 142.4.2.128 (TARGET ADDRESS 4) (36:cc:68:e4:cb:81:12:c5:96:a4:f7:7f:3d:b6:e5:12) (SSH Key Fingerprint 1)
- 192.163.212.110 (TARGET ADDRESS 5) (89:b4:68:71:1f:ce:2a:85:fe:61:0e:d8:22:71:d8:59) (SSH Key Fingerprint 2)
- 142.4.0.84 (TARGET ADDRESS 6) (89:b4:68:71:1f:ce:2a:85:fe:61:0e:d8:22:71:d8:59) (SSH Key Fingerprint 2)
- 142.4.0.45 (TARGET ADDRESS 7) (89:b4:68:71:1f:ce:2a:85:fe:61:0e:d8:22:71:d8:59) (SSH Key Fingerprint 2)

- 142.4.11.163 (TARGET ADDRESS 8)

(89:b4:68:71:1f:ce:2a:85:fe:61:0e:d8:22:71:d8:59) (SSH Key Fingerprint 2)

EXPLANATION OF WEB HOSTING SERVICES

38. Web hosting companies, such as New Fold Digital, maintain servers connected to the Internet. Their customers use these systems to operate websites on the Internet.

39. In general, web hosting companies like Newfold Digital ask each of their customers to provide certain personal identifying information when registering for an account. This information can include the customer's full name, physical address, telephone number and other identifiers, e-mail addresses, and business information. Web hosting companies also may retain records of the length of service (including start date) and types of services utilized. In addition, for paying customers, web hosting companies typically retain information about the customers' means and source of payment for services (including any credit card or bank account number).

40. Web hosting companies' customers place files, software code, databases, and other data on the servers. To do this, customers connect from their own computers to the server computers across the Internet. This connection can occur in several ways. In some situations, it is possible for a customer to upload files using a special web site interface offered by the web hosting company. It is frequently also possible for the customer to directly access the server computer through the Secure Shell ("SSH") or Telnet protocols. These protocols allow remote users to type commands to the web server. The SSH protocol can also be used to copy files to the server. Customers can also upload files through a different protocol, known as File Transfer Protocol ("FTP"). Servers often maintain logs of SSH, Telnet, and FTP connections, showing the dates and times of the connections, the method of connecting, and the Internet Protocol addresses

("IP addresses") of the remote users' computers (IP addresses are used to identify computers connected to the Internet). Servers also commonly log the port number associated with the connection. Port numbers assist computers in determining how to interpret incoming and outgoing data. For example, SSH, Telnet, and FTP are generally assigned to different ports.

41. The servers use those files, software code, databases, and other data to respond to requests from Internet users for pages or other resources from the website. Commonly used terms to describe types of files sent by a server include HyperText Markup Language ("HTML") (a markup language for web content), Cascading Style Sheets ("CSS") (a language for styling web content), JavaScript (a programming language for code run on the client's browser), and image files.

42. Web hosting companies frequently allow their customers to store collections of data in databases. Software running on the web server maintains those databases; two common such programs are named MySQL and PostgreSQL, although these are not the only ones.

43. Web hosting companies sometimes also provide their customers with e-mail accounts; contents of those accounts are also stored on the web hosting company's servers.

44. Web sites deliver their content to users through the Hypertext Transfer Protocol ("HTTP"). Every request for a page, image file, or other resource is made through an HTTP request between the client and the server. The server sometimes keeps a log of all of these HTTP requests that shows the client's IP address, the file or resource requested, the date and time of the request, and other related information, such as the type of Web browser the client uses.

45. Web sites are often known to the outside world by a domain name, such as www.uscourts.gov or www.amazon.com. Domain names must be registered to particular individuals. Sometimes, web hosting companies offer customers the separate service of

registering domain names. When that occurs, web hosting companies typically retain information related to the domain name, including the date on which the domain was registered, the domain name itself, contact and billing information for the person or entity who registered the domain, administrative and technical contacts for the domain, and the method of payment tendered to secure and register the domain name.

46. In some cases, a subscriber or user will communicate directly with a web hosting company about issues relating to a website or account, such as technical problems, billing inquiries, or complaints from other users. Web hosting companies typically retain records about such communications, including records of contacts between the user and the company's support services, as well records of any actions taken by the company or user as a result of the communications.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

47. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Newfold Digital to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

48. Based on the foregoing, I respectfully submit that there is probable cause to believe that the servers and/or IP addresses described in Attachment A were used to further a criminal scheme or artifice to defraud, and I request that the Court issue the proposed search

warrant. Because the warrant will be served on Newfold Digital, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

Steele D. Holland

Steele Holland
Task Force Officer
Federal Bureau of Investigation

Subscribed and sworn to before me on May 18, 2023

/s/ MRC
Mark R. Colombell
United States Magistrate Judge

Honorable Mark R. Colombell
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information and documentation associated with **servers identified by IP addresses:**

- 162.144.78.100 (TARGET ADDRESS 1)
- 162.144.78.186 (TARGET ADDRESS 2)
- 192.163.212.109 (TARGET ADDRESS 3)
- 142.4.2.128 (TARGET ADDRESS 4)
- 192.163.212.110 (TARGET ADDRESS 5)
- 142.4.0.84 (TARGET ADDRESS 6)
- 142.4.0.45 (TARGET ADDRESS 7)
- 142.4.11.163 (TARGET ADDRESS 8)

that are stored at premises owned, maintained, controlled, or operated by Newfold Digital, a company headquartered at 5335 Gate Parkway, 2nd Floor, Jacksonville, Florida 32256.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by New Fold Digital

To the extent that the information described in Attachment A is within the possession, custody, or control of New Fold Digital, regardless of whether such information is located within or outside of the United States, and including any messages, records, files, logs, or information that have been deleted but are still available to New Fold Digital, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Newfold Digital is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. all records or other information pertaining to that account or identifier, including all files, databases, and database records stored by New Fold Digital in relation to that account or identifier;

b. all information in the possession of New Fold Digital that might identify the subscribers related to those accounts or identifiers, including names, addresses, telephone numbers and other identifiers, e-mail addresses, business information, the length of service (including start date), means and source of payment for services (including any credit card or bank account number), and information about any domain name registration;

c. all records pertaining to the types of service utilized by the user,

d. all records pertaining to communications between New Fold Digital and any person regarding the account or identifier, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of wire fraud (18 U.S.C. § 1343) and money laundering (18 U.S.C. § 1956) since January 1, 2020, relating to the development, publishing, advertisement, access, use, administration or maintenance of any website enumerated in Attachment A, including:

1. files, databases, and database records stored by New Fold Digital on behalf of the subscriber or user operating the website, including:

a. programming code used to serve or process requests made via web browsers;

b. HTML, CSS, JavaScript, image files, or other files;

c. HTTP request and error logs;

d. SSH, FTP, or Telnet logs showing connections related to the website, and any other transactional information, including records of session times and durations, log files, dates and times of connecting, methods of connecting, and ports;

e. MySQL, PostgreSQL, or other databases related to the website;

f. email accounts and the contents thereof, associated with the account.

2. Subscriber information related to the accounts established to host the site enumerated in Attachment A, to include:

a. Names, physical addresses, telephone numbers and other identifiers, email addresses, and business information;

b. Length of service (including start date), types of service utilized, means and source of payment for services (including any credit card or back account number), and billing and payment information;

c. If a domain name was registered on behalf of the subscriber, the date that the domain was registered, the domain name, the registrant information, administrative contact information, the technical contact information and billing contact used to register the domain and the method of payment tendered to secure and register the Internet domain name.

d. Any and all available memory capture(s) for servers associated with the IP addresses listed in Attachment A.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC BUSINESS RECORDS PURSUANT TO FEDERAL RULE OF EVIDENCE 902(11)

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by New Fold Digital, and my official title is _____. I am a custodian of records for New Fold Digital. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of New Fold Digital, and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;

b. such records were kept in the ordinary course of a regularly conducted business activity of New Fold Digital; and

c. such records were made by New Fold Digital as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

_____ _____

Date Signature